IEEE P802.11
Wireless LANs

|  |
| --- |
| Resolving LinkID byte order confusion |
| Date: 2014-09-16 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Kazuyuki Sakoda | Sony Corporation | 2-10-1 Osaki Shinagawa-ku, Tokyo, Japan | +81 50 3750 2701 | KazuyukiA.Sakoda at jp dot sony dot com |
| Dan Harkins | Aruba Networks | 1322 Crossman ave, Sunnyvale, California,United States of America | +1 408 227 4500 | dharkins at aruba networks dot com |
|  |  |  |  |  |

Abstract

This submission proposes to resolve the inconsistency of LinkID handling in MTK derivation of SAE.

LinkID (localLinkID/peerLinkID) is defined as an integer identifying peering instance in subclause 13.3.4.1. In general, integers are compared in big endian wise.

However, 802.11REVmc D3.1 includes text specifying the LinkID comparison is to be made in octet stream fashion (in clause 8.2.2). The text in clause 8.2.2 was added as a resolution to CID2426, but the resolution did not change the definition of LinkIDs which causes some inconsistency.

Looking at open source implementation of SAE protocol, LinkIDs are compred in host endian wise (in 16 bit integer).

It is anticipated that the inconsistency will cause more confusion if 802.11REVmc did not indicate clear and consistent definition of LinkIDs and comparison logic.

This submission is a proposal to amend the resolution provided by 11-14/0041r1, and clarify the LinkID comparison logic in natural fashion.

The proposed text changes are based on REVmc D3.1. Corresponding changes to D3.1 are indicated in the following text with “Track Changes” on, to clarify the direction to the editor.

***Instruct the editor to modify section 8.2.2 as indicated:***

**8.2.2 Conventions**

…

Values specified in decimal are coded in natural binary unless otherwise stated. The values in Table 8-1

(Valid type and subtype combinations) are in binary, with the bit assignments shown in the table. Values in

other tables are shown in decimal notation.

For evaluation purposes a nonce is interpreted as a sequence of octets with the most significant

octet first and the most significant bit of an octet first.

…

***Instruct the editor to modify section 13.5.7 as indicated:***

**13.5.7 Keys and key derivation algorithm for the authenticated mesh peering exchange (AMPE)**

…

The temporal key (MTK) shall be derived from the PMK by

MTK 🡨 KDF-X(PMK, “Temporal Key Derivation”, min(localNonce, peerNonce) ||

max(localNonce, peerNonce) || min(localLinkID, peerLinkID) ||

max(localLinkID, peerLinkID) || Selected AKM Suite ||

min(localMAC, peerMAC) || max(localMAC, peerMAC)).

CCMP uses X = 128. The “min” and “max” operations for IEEE 802 addresses are with the address

converted to a positive integer, treating the first transmitted octet as the most significant octet of the integer

as specified in 11.6.1.3 (Pairwise key hierarchy). The “min” and “max” operations for nonces are

encoded as specified in 8.2.2 (Conventions).

**References:**

[1] 802.11REVmc D3.1, August 2014.

[2] Dan Harkins, “Resolution of a Few Security Comments,” 11-14/0041r1